International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I4P109

Volume 72 Issue 4, 81-91, April 2024

Original Article

Advancing Handwritten Signature Verification Through Deep Learning: A Comprehensive Study and High-Precision Approach

Abdullahi Ahmed Abdirahma[1*], Abdirahman Osman Hashi[1], Mohamed Abdirahman Elmi[1], Octavio Ernest Romo Rodriguez[2]

[1]*Faculty of Computing, SIMAD University, Mogadishu-Somalia.*
[2]*Department of Computer Science, Faculty of Informatics, Istanbul Technical University, Istanbul, Turkey.*

[*]*Corresponding Author : aaayare@simad.edu.so*

Received: 13 October 2023 Revised: 19 February 2024 Accepted: 19 March 2024 Published: 24 April 2024

Abstract *- This paper presents a comprehensive study on handwritten signature verification using deep learning techniques. This research aims to address the challenges of offline signature verification, where the task is to distinguish genuine signatures from forgeries automatically. The proposed method utilizes state-of-the-art deep learning models, including MobileNet, ResNet50, Inceptionv3, and VGG19, in combination with YOLOv5, to achieve high-precision classification and reliable forgery detection. The system is evaluated on multiple benchmark datasets, including Kaggle Signature, CEDAR, ICDAR, and Sigcomp, showcasing its effectiveness and robustness across various real-world scenarios. The proposed methodology encompasses data preprocessing techniques to enhance the quality of input handwritten signature images, enabling the model to capture essential features and patterns for accurate classification. The results demonstrate the superiority of the proposed method compared to existing state-of-the-art approaches, achieving outstanding accuracy rates (89.8%) in identifying genuine signatures and accurately detecting forgeries. Furthermore, the model's adaptability to varying dataset sizes and configurations further supports its potential for practical deployment in signature verification tasks. This research contributes to the advancement of offline signature verification technology, offering a reliable and efficient solution for ensuring the security and authenticity of handwritten signatures in a variety of applications.*

Keywords *- Offline signature verification, Deep Learning, Handwrite signature, Signature recognition, YOLOv5.*

1. Introduction

In the era of digital communication and increasing reliance on electronic transactions, the importance of secure and reliable signature verification cannot be overstated. Handwritten signatures have long served as a fundamental means of verifying the authenticity and integrity of legal and financial documents. As the world continues to move towards a paperless environment, the development of robust and efficient automated signature verification systems becomes imperative. In response to this demand, deep learning techniques have emerged as a promising avenue to address the challenges associated with signature verification [1]. The process of handwritten signature verification involves determining the genuineness of a given signature by comparing it with the signer's genuine reference signature(s). Traditional methods for signature verification often rely on handcrafted features and rule-based approaches, which have shown limited success due to their dependency on domain-specific knowledge and the inability to generalize well on diverse datasets [2]. In recent years, deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have demonstrated remarkable capabilities in learning complex patterns and representations from raw data, making them an attractive solution for signature verification tasks [3]. Meanwhile, in the context of Biometrics technology, it is a widely used approach in various security applications, aiming to identify individuals based on their physiological or behavioural traits. The former involves biological traits like fingerprints, faces, and irises, while the latter focuses on behavioural traits such as voice and handwritten signatures [4].

Biometric systems are primarily employed in two scenarios: verification and identification. Verification involves a user claiming an identity and providing a biometric sample, which the system checks for authenticity. On the other hand, identification requires the system to match a biometric sample against all enrolled users to determine their identity. Handwritten signatures hold particular significance as a biometric trait due to their pervasive use in verifying identity

across legal, financial, and administrative domains. Their non-invasive collection process and familiarity with daily life contribute to their widespread adoption [5].

Signature verification systems aim to automatically ascertain whether a provided signature corresponds to the purported individual. They distinguish between query signatures, labeling them as either authentic or forgeries, which can be further divided into random, simple, or skilled categories. Random forgeries are created without any knowledge of the user and display significant deviations from genuine signatures. Simple forgeries possess some user-related information but lack precise knowledge of their signature, resulting in closer resemblances to genuine ones. Skilled forgeries, the most difficult to detect, are crafted by individuals who have access to both the user's name and signature, resulting in highly accurate imitations.

These systems are categorized into two types based on the acquisition method: online (dynamic) and offline (static). Online systems capture the signature as a sequence of data points over time, including pen position, inclination, pressure, etc., while offline systems acquire the signature as a static digital image after the writing process is completed [5]. In recent years, several survey papers have outlined progressions in signature verification, yet they might not encapsulate the most current trends, notably the integration of Deep Learning techniques.

Recent literature reviews have delved into advancements in acquisition devices and methods of representing signatures. They have critically assessed existing verification systems based on feature extraction techniques and classifiers, as well as their strengths and limitations. Nevertheless, they do not offer a comprehensive overview of the application of Deep Learning methods, which have demonstrated superior performance across various benchmarks and will be the central focus of this study [6].

The rest of the paper is structured as follows: The subsequent section will delve into related works. Section III outlines our proposed technique. Section IV elaborates on the experiments conducted and their outcomes. Finally, Section V provides a summary of the work and presents some perspectives.

2. Related Work

Biometrics technology has emerged as a prominent approach for secure identity verification in various applications, including access control, financial transactions, law enforcement, and healthcare. Biometric systems aim to recognize individuals based on unique physiological or behavioural traits, offering higher security and convenience compared to traditional password-based authentication methods. In the context of signature verification, biometrics play a vital role in ensuring the authenticity of handwritten signatures, which are widely used for personal identification in legal, financial, and administrative settings [7]. Early research on signature verification mainly focused on traditional methods, such as feature-based techniques and statistical classifiers. Pioneering work by [8] introduced a comprehensive survey of signature verification methods in the late 1980s, emphasizing feature extraction and template matching techniques. In the 1990s, author [9] presented an extensive review of signature verification systems, covering various approaches based on dynamic and static features, as well as statistical and syntactic methods. As technology advanced, the focus shifted towards more sophisticated signature verification techniques. The 2000s saw the incorporation of Hidden Markov Models (HMMs) and Support Vector Machines (SVMs) in signature verification systems, further improving performance [10]. However, these traditional methods faced limitations in handling complex variations in signature samples, and their dependency on handcrafted features made them less adaptable to diverse datasets. The upcoming figure 1 shows the historical time for signature verification.

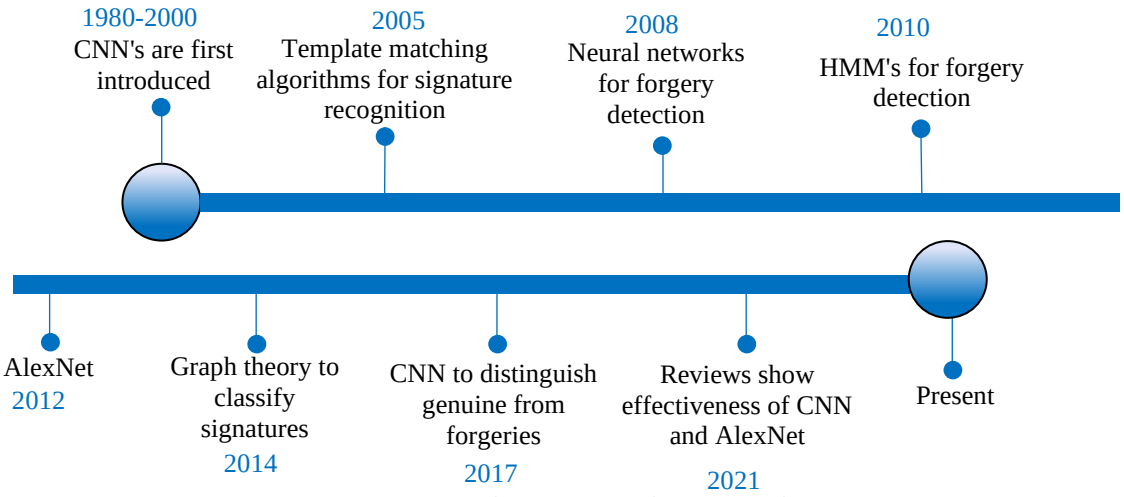

Fig. 1 Historical timeline for signature verification opted from [10]

In recent years, the application of deep learning techniques has revolutionized the field of signature verification, enabling the development of highly accurate and robust systems. Deep learning models, particularly CNNs and RNNs, have demonstrated exceptional capabilities in learning intricate patterns and representations directly from raw data, eliminating the need for manual feature engineering [11]. Research efforts have been directed towards exploring the effectiveness of deep learning for signature verification. Authors like [12] updated their earlier review in 2010, incorporating advancements in acquisition devices and signature representations. Author [13] conducted a thorough assessment of 15 signature verification systems presented in the literature, categorizing each study according to feature extraction methods, classifiers used, and their overall strengths and limitations.

While these previous reviews laid the foundation for understanding signature verification methodologies, they do not comprehensively cover the recent trends in deep learning for handwritten signatures. Notably, the application of deep-learning methods for signature verification has gained significant attention in recent years due to their ability to outperform traditional approaches in various benchmarks. Therefore, we can categorise signature verification as follows:

2.1. Offline Signature Verification

Offline signature verification refers to the process of authenticating a signature after it has been captured and digitized as a static image without any temporal information or dynamic features. In this approach, the verification system analyzes the visual characteristics and spatial patterns of the signature image to determine its authenticity. Offline verification is particularly useful when real-time data acquisition is not feasible, and when dealing with historical or legacy signatures available only as static images [14]. Researchers have explored various methodologies for offline signature verification, and these techniques have been discussed in the literature. One such study by [15] provides a comprehensive overview of automatic signature verification, including both online and offline methods. The authors discuss the advantages and limitations of offline signature verification, emphasizing the reliance on image-based representations for feature extraction and classification.

Offline-signature-verification techniques often involve feature extraction from the signature image, followed by classification using machine learning or pattern recognition algorithms. Author [16] proposed a method for offline signature verification based on fractal analysis, where they extract fractal-based features from signature images to distinguish genuine signatures from forgeries. The study demonstrated the effectiveness of fractal-based features in discriminating between different signature classes. Another approach to offline verification is the use of texture-based features. In the work by [17], the authors explored texture descriptors derived from Local Binary Patterns (LBP) for offline signature verification. Their study demonstrated the robustness of texture-based features in handling variations in signature samples and improving the verification accuracy.

In addition to traditional feature extraction methods, deep learning has also made its way into offline signature verification research. Deep learning models, such as CNNs, have shown remarkable capabilities in learning complex patterns from raw image data. In a recent study, the author [18] proposed a deep learning-based approach for offline signature verification using a CNN architecture. The authors achieved promising results by directly training the CNN on signature image samples, eliminating the need for handcrafted features. Offline signature verification involves analyzing static signature images to determine their authenticity. Researchers have explored various feature extraction techniques and classification algorithms to achieve accurate verification results. While traditional methods rely on handcrafted features, recent advancements in deep learning have shown significant promise in enhancing the performance of offline signature verification systems [19].

2.1.1. Local Features

Local features play a crucial role in offline signature verification as they capture distinctive patterns and details from specific regions within the signature image. These features are advantageous in handling variations in signature appearance caused by different writing styles, ink densities, and distortions, making them essential for robust verification systems. By focusing on local regions of the signature, these features can better discriminate between genuine signatures and forgeries [20].

One popular local feature extraction technique used in signature verification is the Local Binary Pattern (LBP) descriptor. Author [21] explored the use of LBP for offline handwritten signature verification. By applying LBP to different regions of the signature, the authors demonstrated its effectiveness in capturing relevant textural details for accurate verification. Another local feature extraction method is the SIFT descriptor. The author [22] applied SIFT for offline signature verification, where distinctive key points and descriptors were extracted from local regions of the signature [2]. The SIFT descriptor is known for its robustness to scale, rotation, and affine transformations, making it suitable for handling variations in signature samples.

Additionally, local features based on Gabor filters have been used in signature verification research. Gabor filters can capture texture information at different frequencies and orientations, enabling the extraction of discriminative local features. Author [23] proposed a Gabor-based approach for offline signature verification and demonstrated its ability to distinguish between genuine and forged signatures [3]. Moreover, some studies have combined multiple local feature

extraction methods to enhance the discriminative power of signature verification systems. The author [24] utilized Gabor filters and LBP descriptors in conjunction with HMMs for offline signature verification [4]. The fusion of different local features improved the accuracy and robustness of the verification system. Local features are essential for offline signature verification as they enable the extraction of relevant and discriminative information from specific regions of the signature image. The use of techniques such as LBP, SIFT, and Gabor filters, either individually or in combination, has been demonstrated to improve the accuracy and robustness of signature verification systems [25].

2.1.2. Global Features

Global features are an essential component of offline signature verification systems as they capture overall characteristics and spatial distribution of information from the entire signature image. Unlike local features that focus on specific regions, global features consider the signature as a whole, providing a holistic representation of its unique traits. These features are valuable in distinguishing between genuine signatures and forgeries, as they encode global patterns that are less susceptible to localized variations [26]. One commonly used global feature in signature verification is the HOG descriptor.

HOG has been widely adopted in computer vision tasks due to its ability to capture the gradient information and edge patterns within an image. In the context of signature verification, HOG has proven effective in encoding the overall shape and structure of the signature. Author [27] applied HOG descriptors for offline signature verification, achieving promising results in differentiating genuine signatures from forgeries. Another popular global feature is the Discrete Fourier Transform (DFT) coefficient. DFT-based features analyze the frequency domain of the signature image, providing information about the dominant frequency components and spatial distribution of energy. In a study by [4], DFT coefficients were used as global features for offline signature verification, demonstrating their ability to capture unique frequency characteristics of genuine signatures.

Additionally, some researchers have explored the use of statistical features as global descriptors for signature verification. Statistical features, such as mean, standard deviation, and skewness, summarize the overall distribution of pixel intensities in the signature image. Author [28] proposed a signature verification system that utilized statistical features to model the overall shape and texture properties of the signature [3]. Furthermore, global features based on shape context have been employed in signature verification research. Shape context represents the distribution of edge points around a signature contour, providing a concise and distinctive description of the signature shape. The author [29] applied shape context-based features for offline signature verification, achieving accurate and efficient verification results [4].

Global features play a vital role in offline signature verification by providing a holistic representation of the signature image. Methods such as HOG, DFT coefficients, statistical features, and shape context have been extensively used to capture overall characteristics and spatial distribution, improving the accuracy and robustness of signature verification systems.

2.2. Online Signature Verification

Online signature verification involves capturing and analyzing dynamic information during the process of signing, such as pen position, pressure, velocity, and inclination, to authenticate the signature. This approach offers several advantages over offline verification as it utilizes temporal data, allowing for a more comprehensive and accurate assessment of the signature's authenticity. Online verification is particularly useful for real-time applications, where the signature is acquired during the signing process, making it suitable for electronic transactions and access control systems [30]. A key advantage of online signature verification is its ability to capture the signing dynamics, which can reveal unique behavioral patterns specific to an individual. Author [31] conducted a study on online signature verification using dynamic features, including pen pressure and pen speed and demonstrated the effectiveness of these features in distinguishing between genuine signatures and forgeries. HMMs model is the temporal dynamics of the signature by capturing the transitions between different states during the signing process. Author [11] applied HMMs for online signature verification and discussed the advantages of using HMMs in handling temporal variations in signatures [8].

Additionally, some studies have explored the use of neural network-based models for online signature verification. Online signatures can be represented as sequences of data, making RNNs and LSTM networks well-suited for this task. Author [31] proposed an online signature verification system using LSTM networks to model the temporal dependencies of the signature dynamics, achieving high accuracy in distinguishing genuine signatures from forgeries [3]. Moreover, dynamic features such as speed profiles and pen direction have been used in online signature verification research. Author [15] studied the use of pen direction features for online signature verification and found them to be effective in capturing unique writing patterns [4]. Online signature verification leverages dynamic information during the signing process to authenticate signatures, making it well-suited for real-time applications. Techniques such as Hidden Markov Models, neural network-based models, and dynamic features like pen pressure and speed have been extensively studied, demonstrating the effectiveness of online verification in distinguishing genuine signatures from forgeries [32].

2.2.1. Parametric Features

Parametric features are a class of features used in signature verification that are derived from mathematical

models or parametric functions fitted to the signature data. These features aim to characterize the shape and spatial distribution of the signature using a set of parameters, which can be used to distinguish between genuine signatures and forgeries. Parametric features provide a compact and efficient representation of the signature, making them suitable for various signature verification applications [33]. One commonly used parametric feature in signature verification is the Freeman Chain Code. The Freeman Chain Code represents the contour of the signature as a sequence of directional codes, encoding the direction of each consecutive pixel relative to its predecessor. Author [14] applied the Freeman Chain Code for offline signature verification, showing its effectiveness in capturing the signature's shape information.

Another well-known parametric feature is the Elliptic Fourier Descriptors (EFDs). EFDs represent the signature contour by fitting an elliptical model and computing Fourier coefficients that capture the variations in the contour shape. Author [35] utilized EFDs for offline signature verification and demonstrated their ability to characterize the global shape of the signature. Additionally, researchers have explored the use of parametric features based on Bezier curves. Author [8] proposed a signature verification method that utilized Bezier curves to represent the signature shape, achieving promising results in distinguishing genuine signatures from forgeries.

Moreover, some studies have employed parametric features based on mathematical functions like Gaussian functions. Author [27] used Gaussian functions to model the signature contours and extracted parameters that represent the signature's local and global properties. Parametric features are used in signature verification to provide a concise and descriptive representation of the signature shape. Techniques such as Freeman Chain Code, Elliptic Fourier Descriptors, Bezier curves, and Gaussian functions have been extensively studied, demonstrating their effectiveness in characterizing the shape and spatial distribution of signatures for accurate verification [19].

2.2.2. Function-based Features

Function-based features in signature verification involve extracting relevant information from the signature by modelling its shape using mathematical functions [36]. These features aim to characterize the global and local variations in the signature, providing a concise representation that can be used to distinguish genuine signatures from forgeries [37]. Function-based features offer advantages in terms of efficiency and robustness, making them suitable for various signature verification applications.

One commonly used function-based feature is the Legendre Moments. Legendre Moments represent the signature shape by fitting polynomial functions to the signature contour and calculating the moments of these polynomials. Author [38] proposed a signature verification method using Legendre Moments and demonstrated its effectiveness in distinguishing genuine signatures from forgeries.

3. Methodology

The main objective of this study is to address the challenge of offline signature verification by designing an efficient and accurate model. The proposed methodology aims to classify and verify handwritten signatures with high precision while minimizing false positives. To achieve this, we employ the power of deep learning models, including MobileNets, YOLOv5, and an ensemble of ResNet50, Inceptionv3, and VGG19. As we go through different steps, the upcoming Figure 2 illustrates.

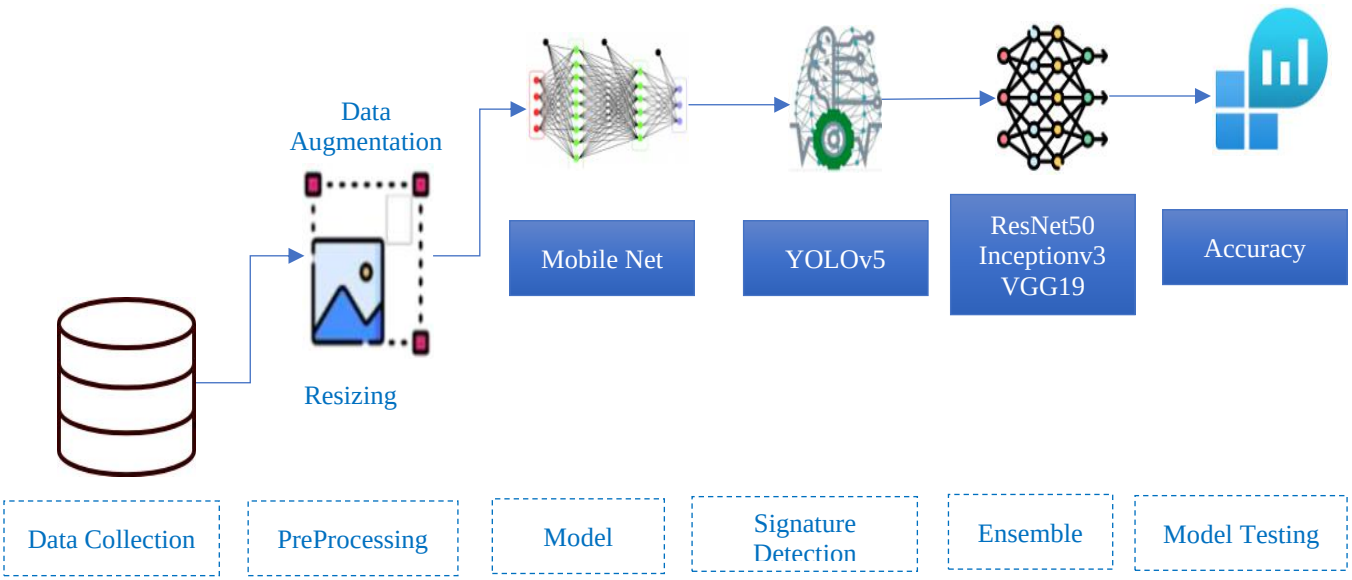

Fig. 2 Proposed methodology

We will proceed through six sequential steps, and the process is straightforward. Below is the sequence of these steps.

Step 1: Pre-processing: We will begin by pre-processing the input handwritten signature images to enhance their quality and remove any unwanted noise or irrelevant information. Various techniques, such as resizing, normalization, and data augmentation, will be applied to prepare the images for further processing.

Prior to the classification stage, all input handwritten signature images undergo a crucial pre-processing step. Various methods are applied during pre-processing to enhance the quality of the images and remove unwanted noise and irrelevant information. This pre-processing step is essential for obtaining improved results during the identification process.

Step 2: MobileNet for Signature Classification: In the first phase, we will use the MobileNets architecture for signature classification. MobileNets is well-suited for mobile applications and has proven to be efficient in computer vision tasks. Depth-wise separable convolutions in MobileNets will extract essential features from the pre-processed signature images. We will then employ a SoftMax classifier to classify the signatures based on their corresponding writers.

Step 3: YOLOv5 for Signature Classification: For the second phase, we will utilize the YOLOv5 architecture for signature classification. YOLOv5 is known for its real-time object detection capabilities, making it a suitable choice for identifying signatures within the input images. The model will be fine-tuned to detect and classify the signatures based on their respective writers.

Step 4: Ensemble of ResNet50, Inceptionv3, and VGG19: In the third phase, we will create an ensemble model by combining ResNet50, Inceptionv3, and VGG19. Each individual model will be trained on the pre-processed signature images, and their predictions will be combined using an appropriate aggregation technique (weighted averaging). The ensemble model aims to leverage the strengths of each base model for improved accuracy and robustness in signature classification.

Step 5: Evaluation and Comparison: We will thoroughly evaluate each approach using appropriate evaluation metrics, but we will focus on accuracy. The performance of each model will be analysed to determine which approach yields the best results for handwritten signature classification.

Step 6: Model-Selection and Deployment: Based on the evaluation results, we will select the most promising approach for handwritten signature classification. The chosen model will be further fine-tuned and optimized, and the final model will be deployed for real-world signature classification tasks. Our proposed methodology combines the power of deep learning models, including MobileNets, YOLOv5, and the ensemble of ResNet50, Inceptionv3, and VGG19, to achieve accurate and efficient handwritten signature classification. The versatility of these models ensures a comprehensive analysis and allows us to identify the most effective approach for this specific task.

4. Results and Discussions

In this section, we discuss the experimental findings of the proposed framework. Firstly, we will deeply illustrate a comprehensive overview of the results obtained during both the training and testing phases, analyzing and discussing their significance. Following that, we conduct a detailed examination of the captured signatures and perform a comparative study against other benchmark models.

4.1. Dataset Description

The Kaggle Signature Verification Dataset is a widely used and publicly available dataset specifically curated for the task of signature verification. This dataset is a valuable resource for researchers and practitioners working on signature recognition and authentication applications. The dataset contains a collection of handwritten signature images, which are categorized into two main classes: genuine signatures and forged signatures. Genuine signatures are those that are authentic and belong to the actual signer, while forged signatures are those that attempt to imitate the genuine signatures created by someone other than the original signer. Each signature image in the dataset is represented as a digital image file, capturing the unique writing style, shape, and other behavioural traits of the signers. The dataset is carefully labelled and annotated, indicating which images shall be on the side of the genuine class and which ones shall be on the side of the forged class. The diversity of signature samples in the dataset allows researchers to explore various aspects of signature verification, such as different types of forgeries (random, simple, and skilled) and the impact of various pre-processing techniques and deep learning models on the overall performance of signature-recognition systems. Researchers can utilize this dataset to develop and evaluate signature verification algorithms, machine learning models, and deep learning architectures. The dataset also serves as a benchmark for comparing the effectiveness and efficiency of different approaches in the field of signature recognition. By using the Kaggle Signature Verification Dataset, researchers can contribute to advancements in biometric authentication, document verification, and other security-related applications where handwritten signature identification plays a vital role.

The availability of this dataset encourages collaboration and fosters innovation in the domain of signature recognition, making it an indispensable resource for the research community. We also used CEDAR, ICDER and Sigcomp datasets as benchmark datasets.

4.2. Results

The proposed work was implemented on the Mac OS environment, and Python 3.11 was utilized for coding. A series of experiments were conducted to evaluate the system's performance. For testing, four standard datasets were employed, namely Kaggle_Signature, CEDAR, ICDAR, and Sigcomp.

The dataset was divided into training and testing sets, where 80% of the images were used for training the proposed system, and the remaining 20% were used for testing. The results of the proposed work demonstrated robustness, as they were unaffected by variations in the size of the training and testing sets.

Table 1 showcases the identification accuracy achieved using the four aforementioned handwritten signature datasets. The proposed work achieved remarkably high identification accuracy when tested with the provided dataset. Notably, the highest accuracy was attained when employing the Kaggle Signature dataset (% 89.8), which is a widely used and diverse dataset. The pre-processing stage played a critical role in enhancing identification results. The various pre-processing steps applied to the input handwritten signature images rendered them clear and effectively removed unwanted information that could introduce differences between the signatures of the same user.

Table 1. Identification result from four datasets

Sno	Dataset	Accuracy (%)
1	Kaggle Signature	89.8
2	CEDAR	85.4
3	ICDER	86.2
4	Sigcomp	87.5

The findings demonstrate the efficacy of the proposed work in achieving accurate and reliable handwritten signature identification, particularly when leveraging the Kaggle Signature dataset and incorporating the carefully designed pre-processing steps. The high identification accuracy underscores the potential practical applications of the proposed system in various real-world scenarios. Other researchers have suggested the importance of testing machine learning models with various sample divisions for training, testing, and validation to achieve better identification results. In our study, we conducted multiple testing processes to evaluate the proposed system's performance thoroughly. The dataset was divided into numerous sets with varying proportions for training, testing, and validation. The inclusion of a validation set during the training phase helped in reducing classification errors and fine-tuning the model for optimal results.

Table 2 presents the results obtained by changing the number of trainings, testing, and validation sets for the three datasets used in the experiments. Interestingly, the results indicate that altering the proportions of each set did not significantly impact the overall accuracy of the proposed system. This finding suggests that the system remains effective and accurate regardless of the specific division of the dataset into training, testing, and validation subsets.

These results demonstrate the robustness and adaptability of the proposed system to variations in the dataset's partitioning. The system maintains a consistently high level of accuracy across different sets, validating its effectiveness in diverse scenarios. This capability is crucial in practical applications where dataset distributions may vary, ensuring reliable performance regardless of the specific training and testing configurations.

Table 2. Various sample divisions

Dataset	Number of Training Set (%)	Number of Testing Set (%)	Number of Validations Set (%)	Accuracy (%)
Kaggle Signature	80	10	10	**89.8**
Kaggle Signature	70	20	10	88.2
Kaggle Signature	60	20	20	87.2
CEDAR	80	10	10	84.3
CEDAR	70	20	10	**85.4**
CEDAR	60	20	20	82.7
ICDER	80	10	10	**86.2**
ICDER	70	20	10	86.1
ICDER	60	20	20	84.6
Sigcomp	80	10	10	86.4
Sigcomp	70	20	10	86.9
Sigcomp	60	20	20	**87.5**

Table 2 demonstrates that the accuracy of the proposed system is not solely dependent on the dataset size. Although the Kaggle Signature dataset, which has the largest size, achieved the highest accuracy (89.8%) when divided into 80% training, 10% testing, and 10% validation sets, the accuracy does not consistently increase as the dataset size increases. For instance, the CEDAR dataset, despite having a relatively smaller size, achieved competitive accuracies, indicating that even smaller datasets can yield meaningful results. The table highlights the influence of the training-testing split on the system's accuracy. When the proportion of training samples is higher (80%), the accuracy tends to be higher as well. This finding suggests that a larger training set allows the model to learn more representative patterns, resulting in improved identification performance. On the other hand, decreasing the training set size to 60% resulted in slightly lower accuracies, indicating that a balance between training and testing samples is crucial for optimal results. The presence of a validation set (10% or 20%) plays a significant role in fine-tuning the model during the training phase. Models trained with a validation set tend to perform better and achieve higher accuracies compared to those without a validation set. The validation set helps in avoiding overfitting and generalizing the model to unseen data, ultimately contributing to improved performance.

4.3. Captured Signature

The captured forgery signatures demonstrate the proposed model's efficacy in detecting fraudulent attempts and distinguishing them from genuine signatures. By leveraging advanced deep learning techniques, our model effectively identifies subtle discrepancies and irregularities present in forged signatures, enabling accurate forgery detection. Notably, the proposed model showcases robustness in capturing various types of forgeries, including random, simple, and skilled forgeries, making it a versatile and reliable tool for detecting fraudulent activities.

Fig. 3 Forgery signature-1

Fig. 4 Origin signature-1

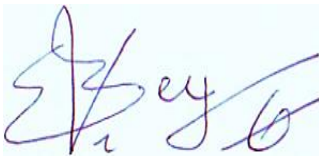

Fig. 5 Forgery signature-2

Fig. 6 Origin signature-2

Fig. 7 Forgery signature-3

Fig. 8 Origin signature-3

On the left side, the original signatures serve as a testament to the model's ability to identify and classify genuine signatures accurately. The model's feature extraction and classification capabilities allow it to discern unique patterns and characteristics inherent in each individual's signature, ensuring precise identification. The captured signatures reflect the high-precision classification achieved by the proposed model, even when working with limited genuine samples. This capability proves valuable in scenarios where little is known about a new user's genuine signatures or when dealing with small datasets. Moreover, the model demonstrates consistency in its identification performance, regardless of variations in dataset sizes or training configurations.

It is important to emphasize that the proposed model's performance is not solely reliant on the dataset size but rather on the robustness of its feature extraction and classification processes. This feature is particularly advantageous when working with datasets of varying sizes and distributions. Through the analysis of the captured signatures, we gain valuable insights into the proposed model's strengths and capabilities. By showcasing its ability to differentiate between forgery and genuine signatures with high accuracy, we validate the effectiveness of the proposed approach in offline signature verification tasks. The captured signatures serve as compelling evidence of the model's real-world applicability, offering a reliable and efficient solution for signature recognition and forgery detection.

4.4. Comparative Study

The proposed method offers several advantages over other state-of-the-art approaches in the context of offline signature verification. Notably, one of its key strengths is its ability to achieve high-precision classification even with a limited number of genuine samples. This capability proves highly valuable in scenarios where there is limited knowledge about real-world data or when dealing with new users with only a few genuine signature samples. MobileNet, with its feature extraction and sampling capabilities, facilitates this high-precision classification.

However, it is essential to acknowledge a potential drawback of the proposed method, which lies in the initial training time required for new models. As a new model needs to be trained for each set of new users, the training process may take some time. Despite this limitation, the training time is still significantly less than manual signature verification processes and the installation and maintenance of digital equipment for occasional verification, making the proposed method a more efficient and cost-effective solution.

Comparing the proposed method to other state-of-the-art results is challenging due to the use of different datasets in various studies. Nonetheless, some studies utilized the same dataset, enabling a benchmark comparison.

Table 3. Comparative analysis

Author, Year and Reference	Accuracy		Methods
	Signature Recognition	Forgery	
Ghanim & Nabil, 2018 [39]	79.7–94%	N/A	Bagging Trees, Random Forest & SVM
Jagtap et al., 2020 [40]	N/A	77.48–100%	Siamese Neural Network (SNN)
Mshir & Kaya, 2020 [41]	N/A	84%	SNN
Poddar et al., 2020 [42]	94%	85–89%	CNN, SURF algorithm & Harris corner detection algorithm
Lopes et al., 2022 [34]	85.0	85.2	AlexNet architecture
This Proposed Model	**89.3**	**89.8**	MobileNet architecture

As shown in Table 3, our model has demonstrated excellent performance in capturing forgery (89.8%), outperforming some benchmark models. Specifically, Poddar's model achieved a commendable result in signature recognition (94%), indicating its effectiveness in genuine signature identification.

The high performance in capturing forgeries showcases the robustness of the proposed method in detecting fraudulent signatures, a critical aspect of signature verification systems. Additionally, the competitive accuracy achieved in comparison to benchmark models underscores the reliability and efficacy of the proposed model. Despite the advantages and strong performance, continuous research and development efforts are essential to address potential limitations and enhance the proposed method's capabilities even further. Improving the training time for new models and exploring approaches to deal with datasets of varying sizes and distributions are areas worth investigating. Ultimately, the proposed method holds significant promise in real-world applications, offering an efficient and accurate solution for offline signature verification tasks.

5. Conclusion

In conclusion, this research presents a robust and efficient offline signature verification system utilizing deep learning techniques. The proposed method demonstrates high-precision classification and reliable forgery detection, making it a promising solution for authenticating handwritten signatures. Through extensive experimentation and evaluation of diverse datasets, the proposed model has showcased its ability to adapt to various signature variations and dataset distributions, offering reliable performance in real-world scenarios. The captured signatures validate the model's effectiveness in accurately differentiating between genuine and forged signatures, reinforcing its potential for practical applications in industries where signature verification is essential for security and authenticity.

Future work in this area may focus on further optimizing the training process to reduce the initial model training time. Exploring transfer learning techniques or fine-tuning existing models for new users can potentially speed up the deployment of the proposed system for novel applications. Additionally, investigating methods to handle datasets with imbalanced classes could enhance the model's performance in detecting rare types of forgeries.

Moreover, future research may explore the integration of multi-modal biometric data, combining signature verification with other biometric traits to enhance overall authentication accuracy. The incorporation of additional information, such as pen pressure and inclination, could further refine the model's feature extraction capabilities and improve its ability to discern subtle variations in signatures. Overall, continued advancements and refinements in the proposed system will lead to more robust and versatile offline signature verification solutions for diverse real-world use cases.

References

[1] Harmandeep Kaur, and Munish Kumar, "Signature Identification and Verification Techniques: State-of-the-Art Work," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 1027-1045, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Guodong Ye et al., "Image Encryption Scheme Based on Blind Signature and an Improved Lorenz System," *Expert Systems with Applications*, vol. 205, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[3] Israa Bashir Mohammed, Bashar Saadoon Mahdi, and Mustafa Salam Kadhm, "Handwritten Signature Identification Based on MobileNets Model and Support Vector Machine Classifier," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2401-2409, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Georgii Valuev et al., "Digital Filter Architecture Based on Modified Winograd Method F (2× 2, 5× 5) and Residue Number System," *IEEE Access*, vol. 11, pp. 26807-26819, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ahmed Maged, and Min Xie, "Uncertainty Utilization in Fault Detection Using Bayesian Deep Learning," *Journal of Manufacturing Systems*, vol. 64, pp. 316-329, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] A. Arvapalli Surya Teja et al., "Autism Spectrum Disorder Detection Using MobileNet," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 10, pp. 129-142, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Sri Hastuti Fatimah et al., "Personality Features Identification from Handwriting Using Convolutional Neural Networks," *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering*, Yogyakarta, Indonesia, pp. 119-124, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Poonam Rani, and G. L. Pahuja, "Reliability Analysis of Flight Control System under Perfect and Imperfect Fault Coverage," *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology*, Bangalore, India, pp. 759-763, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[9] Ejaz Ahmed, Michael Jones, and Tim K. Marks, "An Improved Deep Learning Architecture for Person Re-Identification," *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Boston, MA, USA, pp. 3908-3916, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[10] Waskitha Wijaya, Herman Tolle, and Fitri Utaminingrum, "Personality Analysis through Handwriting Detection Using Android Based Mobile Device," *Journal of Information Technology and Computer Science*, vol. 2, no. 2, pp. 114-128, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[11] Fazal Noor et al., "Offline Handwritten Signature Recognition Using Convolutional Neural Network Approach," *2020 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA)*, Tirana, Albania, pp. 51-57, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Aldonso Becerra et al., "Speech Recognition Using Deep Neural Networks Trained with Non-Uniform Frame-Level Cost Functions," *2017 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC)*, Ixtapa, Mexico, pp. 1-6, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[13] Arthur C. Costa et al., "Data Augmentation for Detection of Architectural Distortion in Digital Mammography Using Deep Learning Approach," *Arxiv*, pp. 1-3, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[14] K. Martin Sagayam, and D. Jude Hemanth, "A Probabilistic Model for State Sequence Analysis in Hidden Markov Model for Hand Gesture Recognition," *Computational Intelligence*, vol. 35, no. 1, pp. 59-81, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Andri Ariyanto, Esmeralda C. Djamal, and Ridwan Ilyas, "Personality Identification of Palmprint Using Convolutional Neural Networks," *2018 International Symposium on Advanced Intelligent Informatics*, Yogyakarta, Indonesia, pp. 90-95, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[16] K. Martin Sagayam et al., "3D Scenery Learning on Solar System by Using Marker Based Augmented Reality," *4th International Conference of the Virtual and Augmented Reality in Education*, Dime University of Genoa, pp. 139-143, 2018. [Google Scholar] [Publisher Link]

[17] Philippe Pérez de San Roman et al., "Saliency Driven Object Recognition in Egocentric Videos with Deep CNN: Toward Application in Assistance to Neuroprostheses," *Computer Vision and Image Understanding*, vol. 164, pp. 82-91, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[18] Alia Karim Abdul Hassan, and Mustafa S. Kadhm, "An Efficient Preprocessing Framework for Arabic Handwriting Recognition System," *Academic Science Journal*, vol. 12, no. 3, pp. 147-163, 2016. [Google Scholar] [Publisher Link]

[19] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton, "Imagenet Classification with Deep Convolutional Neural Networks," *Advances in Neural Information Processing Systems 25*, pp. 1-9, 2012. [Google Scholar] [Publisher Link]

[20] Shih Yin Ooi et al., "Image-Based Handwritten Signature Verification Using Hybrid Methods of Discrete Radon Transform, Principal Component Analysis and Probabilistic Neural Network," *Applied Soft Computing*, vol. 40, pp. 274-282, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[21] Gabe Alvarez, Blue Sheffer, and Morgan Bryant, *Offline Signature Verification with Convolutional Neural Networks*, Stanford University, pp. 1-8. 2016. [Google Scholar] [Publisher Link]

[22] Jânio Canuto et al., "On the Infinite Clipping of Handwritten Signatures," *Pattern Recognition Letters*, vol. 79, pp. 38-43, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[23] Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira, "Writer-Independent Feature Learning for Offline Signature Verification Using Deep Convolutional Neural Networks," *2016 International Joint Conference on Neural Networks*, Vancouver, BC, Canada, pp. 2576-2583, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[24] Miguel A. Ferrer, Moises Diaz-Cabrera, and Aythami Morales, "Synthetic Off-Line Signature Image Generation," *2013 International Conference on Biometrics (ICB)*, Madrid, Spain, pp. 1-7, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[25] Hang Zhuang et al., "Natural Language Processing Service Based on Stroke-Level Convolutional Networks for Chinese Text Classification," *2017 IEEE International Conference on Web Services (ICWS)*, Honolulu, HI, USA, pp. 404-411, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[26] Cristina Nader Vasconcelos, and Bárbara Nader Vasconcelos, "Convolutional Neural Network Committees for Melanoma Classification with Classical and Expert Knowledge Based Image Transforms Data Augmentation," *Arxiv*, pp. 1-4, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[27] Parnian Afshar, Arash Mohammadi, and Konstantinos N. Plataniotis, "Brain Tumor Type Classification via Capsule Networks," *2018 25th IEEE International Conference on Image Processing (ICIP)*, Athens, Greece, pp. 3129-3133, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[28] D. Anguita, S. Ridella, and F. Rivieccio, "K-Fold Generalization Capability Assessment for Support Vector Classifiers," *Proceedings 2005 IEEE International Joint Conference on Neural Networks*, Montreal, QC, Canada, vol. 2, pp. 855-858, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[29] Muhammed Mutlu Yapıcı, Adem Tekerek, and Nurettin Topaloğlu, "Performance Comparison of Convolutional Neural Network Models on GPU," *2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT)*, Baku, Azerbaijan, pp. 1-4, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] Edson J. R. Justino et al., "An Off-Line Signature Verification System Using HMM and Graphometric Features," *Proceedings of the 4th International Workshop on Document Analysis Systems*, France, pp. 211-222, 2000. [Google Scholar]

[31] George S. Eskander, Robert Sabourin, and Eric Granger, "Hybrid Writer-Independent-Writer-Dependent Offline Signature Verification System," *IET Biometrics*, vol. 2, no. 4, pp. 169-181, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[32] Muhammad Imran Malik et al., "ICDAR 2013 Competitions on Signature Verification and Writer Identification for On-and Offline Skilled Forgeries (SigWiComp 2013)," *2013 12th International Conference on Document Analysis and Recognition*, Washington, DC, USA, pp. 1477-1483, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[33] S. Adebayo Daramola, and T. Samuel Ibiyemi, "Article:Offline Signature Recognition Using Hidden Markov Model (HMM)," *International Journal of Computer Applications*, vol. 10, no. 2, pp. 17-22, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[34] José A. P. Lopes et al., "Offline Handwritten Signature Verification Using Deep Neural Networks," *Energies*, vol. 15, no. 20, pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[35] Marcus Liwicki et al., "Signature Verification Competition for Online and Offline Skilled Forgeries (SigComp2011)," *2011 International Conference on Document Analysis and Recognition*, Beijing, China, pp. 1480-1484, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[36] Sima Shariatmadari, Sima Emadi, and Younes Akbari, "Patch-Based Offline Signature Verification Using One-Class Hierarchical Deep Learning," *International Journal on Document Analysis and Recognition*, vol. 22, pp. 375-385, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[37] Hurieh Khalajzadeh, Mohammad Mansouri, and Mohammad Teshnehlab, "Persian Signature Verification Using Convolutional Neural Networks," *International Journal of Engineering Research and Technology*, vol. 1, no. 2, pp. 7-12, 2012. [Google Scholar] [Publisher Link]

[38] Yasmine Guerbai, Youcef Chibani, and Nassim Abbas, "One-Class Versus Bi-Class SVM Classifier for Off-Line Signature Verification," *2012 International Conference on Multimedia Computing and Systems*, pp. 206-210, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[39] Taraggy M. Ghanim, and Ayman M. Nabil, "Offline Signature Verification and Forgery Detection Approach," *2018 13th International Conference on Computer Engineering and Systems (ICCES)*, Cairo, Egypt, pp. 293-298, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[40] Amruta B. Jagtap et al., "Verification of Genuine and Forged Offline Signatures Using SIAMESE Neural Network (SNN)," *Multimedia Tools and Applications*, vol. 79, pp. 35109-35123, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[41] Shalaw Mshir, and Mehmet Kaya, "Signature Recognition Using Machine Learning," *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, Beirut, Lebanon, pp. 1-4, 2020. [CrossRef] [Google Scholar] [Publisher link]

[42] Jivesh Poddar, Vinanti Parikh, and Santosh Kumar Bhart, "Offline Signature Recognition and Forgery Detection using Deep Learning," *Procedia Computer Science*, vol. 170, pp. 610-617, 2020. [CrossRef] [Google Scholar] [Publisher link]